IN THE CLAIMS

1. (Currently Amended) A method, comprising:

determining a private key for a first network based on at least one security value associated with a second network, wherein the private key refers to a key that, once calculated, is not shared with another device; and

establishing a plurality of sessions between a mobile terminal and the first network using the private key.

2. (Previously Presented) The method of claim 1, wherein the second network is a cellular network and the first network is a wireless local area network, and wherein determining the private key comprises determining the private key based on a shared secret data key associated with the cellular network.

3. (Original) The method of claim 2, wherein determining the private key based on the shared secret data key comprises applying a root key, an electronic serial number associated with the mobile terminal, and a network-supplied random value to a Cellular Authentication and Voice Encryption (CAVE) algorithm to generate the private key.

4. (Original) The method of claim 2, wherein determining the private key further comprises populating the private key with a cryptographic transform of the shared secret data key.

5. (Previously Presented) The method of claim 1, wherein the second network is a cellular network having an associated authentication center and the first network is a wireless

local area network, and wherein determining the private key comprises determining the private key based on one or more random challenges generated by the authentication center associated with the cellular network.

6. (Original) The method of claim 5, wherein the cellular network is a code division multiple access (CDMA) network, wherein determining the private key comprises determining one or more responses associated with the one or more challenges based on the shared secret data key associated with the CDMA network and combining the determined one or more responses to form the private key.

7. (Original) The method of claim 1, further comprising determining at least one session key based on the determined private key.

8. (Original) The method of claim 1, wherein establishing the plurality of sessions comprises authenticating the mobile terminal to the first network for each of the plurality of sessions.

9. (Original) The method of claim 7, wherein authenticating the mobile terminal to the first network comprises:

receiving a challenge from the first network; and

transmitting a response associated with he received challenge, wherein the response is calculated based on the private key.

10. (Original) The method of claim 1, wherein establishing the plurality of sessions comprises determining a session key for each of the plurality of sessions based on the private key.

11. (Currently Amended) A method, comprising:

receiving at least one security value associated with a cellular network;

determining a private key for a wireless local area network based on the security value associated with the cellular network, wherein the private key refers to a key that, once calculated, is not shared with another device; and

allowing establishment of a plurality of sessions between a mobile terminal and the wireless local area network using the private key.

12. (Original) The method of claim 11, wherein the cellular network is a code division multiple access (CDMA) network, and wherein receiving the at least one security value comprises receiving a shared secret data key associated with the CDMA network and wherein determining the private key comprises using the shared secret data key as the private key.

13. (Original) The method of claim 12, wherein determining the private key comprises populating the private key with a cryptographic transform of the shared secret data key.

14. (Original) The method of claim 12, wherein receiving the shared secret data key comprises receiving the shared secret data key over a Signaling System 7 (SS7) protocol.

15. (Original) The method of claim 12, wherein the cellular network is a code division multiple access (CDMA) network having an associated authentication center, and wherein receiving at least one security value comprises receiving one or more responses associated with one or more challenges that are generated by the authentication center associated with the CDMA network.

16. (Original) The method of claim 15, wherein receiving the one or more responses comprises receiving the one or more responses over a Signaling System 7 (SS7) protocol.

17. (Original) The method of claim 15, further comprises receiving the one or more challenges from the authentication center and providing the one or more challenges to the mobile terminal.

18. (Original) The method of claim 17, wherein providing the one or more challenges to the mobile terminal comprises providing the one or more challenges over an Extensible Authentication Protocol.

19. (Original) The method of claim 17, wherein determining the private key comprises combining the one or more responses.

20. (Currently Amended) A method, comprising:

receiving, at a server that is associated with a wireless local area network, at least one security value associated with a cellular network;

determining, using the server, a private key based on the at least one security value;

determining, at a mobile terminal, a private key based on the at least one security value associated with the cellular network, wherein the private key refers to a key that, once calculated, is not shared with another device; and

allowing establishment of a plurality of sessions between the mobile terminal and the wireless local area network using the private key determined by the mobile terminal.

21. (Original) The method of claim 20, wherein receiving the at least one security value comprises receiving a shared secret data key associated with the cellular network and wherein determining, at the server, comprises determining the private key based on the shared secret data key.

22. (Original) The method of claim 20, wherein receiving the at least one security value comprises receiving one or more random challenges generated by an authentication center associated with the cellular network and wherein determining, at the server, comprises determining the private key based on one or more signed responses associated with the respective one or more challenges.

23. (Original) The method of claim 20, further comprises transmitting messages between the server and the mobile terminal using an Extensible Authentication Protocol.

24. (Original) The method of claim 20, wherein determining, at a mobile terminal, the private key based on the at least one security value associated with the cellular network

comprises determining the at least one security value associated with at least one of a CDMA network, TDMA network, GSM network, OFDMA network, and AMPS network.